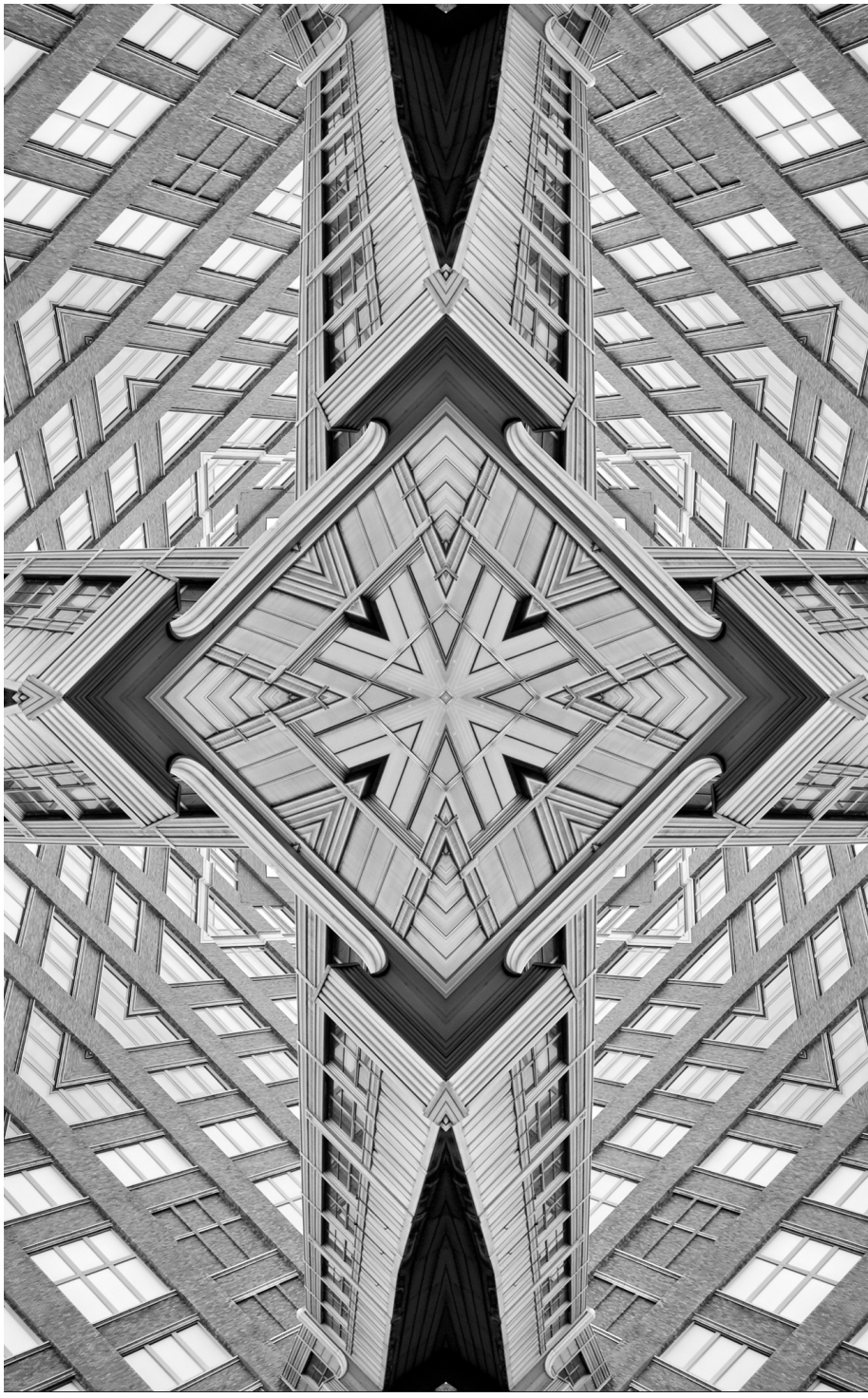
OBSERVER RESEARCH FOUNDATION

Issue Brief

ISSUE NO. 681
DECEMBER 2023



Crime and Punishment in the Metaverse: A Primer

Shravishtha Ajaykumar

Abstract

Immersive technology is a key part of the emerging Web 3.0. A prominent aspect of this evolution of the World Wide Web is the Metaverse, which aims to build a fully immersive and self-sustaining virtual shared space for humans to use as they would the physical world in all aspects of life. Existing concerns and debates on privacy, user protection, and the ethics of monetising platforms also extend to the Metaverse. This brief discusses the three main areas of potential user safety issues in the Metaverse: avatar use; government-, business-, and peer-induced censorship; and decentralised finance and virtual asset ownership. It also explores the existing regulations pertaining to privacy and user safety, and how these can inspire a Metaverse-specific directive.

Attribution: Shravishtha Ajaykumar, "Crime and Punishment in the Metaverse: A Primer," *ORF Issue Brief No. 681*, December 2023, Observer Research Foundation.

Introduction

The first generation of the World Wide Web, termed Web 1.0, was characterised by open protocols, open-source codes, and shared forums.[1] Web 2.0[a] emerged in the early 2000s, with content-focused websites and the rise of the mobile internet.[2] However, platforms like Facebook, Google, and Twitter, which were controlled by large companies, created a virtual monopoly over the space. The emerging Web 3.0 aims to establish decentralised workspaces and promises fully immersive experiences through the Metaverse.[3]

The Metaverse is an extended form of the Cyber-Physical Social System, in which physical systems, human society, and cyber systems are interconnected with complex interactions.[4] It is anticipated that the Metaverse will fully evolve through four broad stages[5]:

Stage 1: Virtual reality (VR) technology will allow users to experience visuals and sounds in the Metaverse. This stage is primarily dominated by gaming companies. The advent of blockchain, cryptocurrencies, and non-fungible tokens (NFTs) have also contributed to the advancement of the Metaverse, with an increased interest in owning unique digital assets based in blockchain, such as 'skins' for avatars in gaming worlds.[6]

Stage 2: The second stage looks to further sensory immersion through a combination of movement and touch-enhancing hardware, such as haptic suits,[7] to let the wearer simulate movement.[8]

Stage 3: The third stage seeks to use what is occasionally called advanced VR to simulate real-world experiences by transferring information directly to the brain via neural signals.[9] One example would be using virtual environments and reality for pain management for clinical patients.[10] Collecting neural information in response to stimuli presented in VR, though not common practice, is another developing area (and is currently being explored by companies such as Neuralink[11]). The overarching goal is to "transport consciousness" without transporting the body.[12]

Stage 4: The final foreseeable stage of the Metaverse would be indistinguishable from the physical world, with advanced neurotechnology merging the experience of a virtual and physical world completely.[13]

a Often used to describe the earliest form of internet networks, with a focus on fetching and providing data.

Introduction

The Metaverse is currently in the first stage, with some early adopters, such as gaming companies and some technology service providers (for instance, Samsung, Meta, and Apple Inc.), using the platform as a market while moving into the second stage.[14] The Metaverse was valued at US$120 billion in mid-2022 and is projected to grow to about US$5 trillion by 2030.[15]

Despite its potential and promise, a fully immersive and unregulated space like the Metaverse also risks criminal activity and misconduct.[16] Notably, threats in the virtual world will also severely affect physical infrastructures, personal safety, and human society. It is thus necessary to establish regulations at a global and Metaverse level to tackle such issues.

This brief discusses the three main areas of potential safety issues in the Metaverse: avatar use; government-, business-, and peer-induced censorship; and decentralised finance and virtual asset ownership. Further, it explores how such issues can be combatted through regulatory tools, global cooperation, and ethical guidelines.

> "The emerging Web 3.0 aims to establish decentralised workspaces and promises fully immersive experiences through the Metaverse."

Potential Crime and Misconduct in the Metaverse

As technology evolves, the potential for criminal behaviour and misconduct also increases. The internet has been a prominent platform for violence and crime, especially against vulnerable minorities, due to the relative anonymity it provides users.[17] Internet users already submit private data for better algorithm-driven experiences.[18] Given the immersive experience in the Metaverse, privacy issues will likely expand with new forms of data being generated at a scale that is currently difficult to comprehend in entirety.[19]

The Metaverse's immersive nature is also a factor to consider, as information on involuntary user actions—such as eye movements, palm and fingerprint movements, minor body movements, and hormone activity—could also be collected and used by the platform.[20] Tech firm Meta has already indicated it intends to monetise behavioural and biometric data collected in the Metaverse.[21] One example of this is the use of the eye in the Metaverse,[22] where the system uses examples of eye movement based on actions made by a set of "virtual eyes" to guess what a person is doing or looking at.

Similar systems are also used to track behavioural responses, giving rise to concerns related to privacy and the ethics of using such technology.[23] Since most of the Metaverse is currently contained on gaming or gamified platforms, including Sandbox[b] and Roblox,[c] it holds a greater appeal for a younger audience, including minors.[24] The younger audience, especially minors, are more vulnerable and need protection against malicious and predatory behaviour from companies and other users.[25]

These gaming platforms utilise large language models, more popularly known as machine learning (ML), to understand and respond to users' actions. Such models are often used to enhance game difficulty levels, but can also be used to exploit users into submitting data or making false purchases. There is already widespread scepticism around the accuracy of such ML systems, but without any ethical guidelines and deployment regulations, the implementation of exploitative ML, which encourages user spending and reduces data privacy, by companies is inevitable.[26] Meta (and indeed many other tech firms) has been granted many patents regarding the use of technology to track biometric data like eye movements,[27] but it is yet to discuss this in terms of the intended use or purpose limitation and the ethical guidelines they have or will adopt for such use.

b An online gaming platform that is hosted on a Metaverse-like platform for an immersive experience.
c A gaming platform that can be used on smartphones and extends into Metaverse-like platforms.

In addition to platform-based privacy concerns, there is also a danger of cyber-assisted crime and radicalisation. Platforms like Reddit have already been linked to radicalising users and leading them to partake in online and offline criminal activity.[28] On decentralised platforms, tracking mobilisers will be even more arduous, increasing the need for regulation accountability.

User Avatars

Avatars are intangible representations of users on platforms, including static pictures, illustrated representations (like bitmojis), or humanoid representations. Users' avatars in the Metaverse function as an access point. These avatars also provide users with a mask to help with interaction, information dissemination, and perceived cultural unity.[d] With the Metaverse's decentralised foundation, the lack of singular ownership creates an accountability challenge as individual avatars do not come under any single jurisdiction, as humans do in the physical world.

In the Metaverse, avatars could be involved in altercations that, in the physical world, would be a breach of tort or criminal law.[e,29] One potential malicious use is defamation. Creating avatars under the guise of another personality is not illegal but can misrepresent the personality, contributing to distrust, dissatisfaction, and nuisance for other users.

Since gaming companies currently dominate the Metaverse, many actions in the virtual space that may be part of acceptable gaming culture (such as theft, robbery, and shooting in first-person shooting games, may translate to assault in the physical world.[30] This would create the need for nuanced regulations differentiating assault from acceptable contextual behaviour. This, in turn, would require the Metaverse to grant rights to the avatars along the lines of civil and human rights. These protections would also require avatars to be held accountable as individuals for their actions, indicating the attribution of a legal persona to each avatar within a legal system that allows for action against offending entities.

Avatars enable users to create identities that may differ from their own in the physical world, allowing them to change their behaviour due to the relative anonymity, and enabling individuals to act in ways that would not be possible

d Allowing users to lose identity indicators like nationality, race, and gender, and present themselves as citizens of the internet.

e Criminal law governs illegal acts and crimes such as assault, murder, burglary, or sexual violence.

or acceptable in the offline world.[31] The avatar's anonymity in the Metaverse, therefore, could inculcate a culture of reduced accountability, allowing actors with malicious intent to exercise individual power at the expense of community safety.

It is difficult to attribute legal liability to an avatar and its user, especially since avatars may possess artificial intelligence (AI) or ML capabilities, such as character merchandising.[f,32] Although programmed by a human or set of humans, such avatars will also learn from interactions, diffusing the accountability attributed to a single user with each interaction as time progresses. This legal personality could be bestowed through registration, with each individual registering only one avatar in the Metaverse. In the case of AI and ML, this could be furthered by treating avatars like companies (similar to how companies are treated as individual entities in accounting and business law). Arguments in favour of attributing a legal personality to robots can also be expanded to Metaverse avatars.[33] Indeed, avatars can commit multiple types of crimes and atrocities beyond just user–to–user interaction. For instance, the Metaverse can act as a platform for avatars to sell stolen intellectual property from outside the Metaverse, similar to how stolen images of Birkin bags were sold as NFTs.[34]

In many instances in the physical world, to avoid conflict in fraud and financial fleecing, the legal entity of a corporation is treated as separate from the proprietor.[35] In the Metaverse, it will be necessary to distinguish avatars from their users, especially in cases where avatars are created by programmers for commercial purposes. It would be important to hold the actions of these avatars accountable, even if based on AI and ML, without necessarily incriminating the programmer[36]

In the Metaverse, identity is an aspect of humanity that will have value. Whether in terms of cultural, social, or any other facets of identity that one may choose to align with, this primarily includes individual identity. Defamation and identity theft can lead to incrimination and liability for those unaware of their identity being misused. In the Metaverse, the concern around identity and representation is enhanced, as there is no way to confirm virtual identity without crossing lines of data privacy. Thus, to limit identity theft and the loss of data privacy in this area, platforms need to intervene. Creating avatar incorporation and registration processes (to make avatars contractual and permanent obligations) is one way to challenge this.[37]

f Adaptation or creation of a fictional character that may resemble real personas, used to interact with real people for purposes of selling, advertising, and influencing.

Sexual harassment and identity theft, already common on social media, will likely worsen in the Metaverse. In the Metaverse, harassment can include theft of intellectual property, personal imagery for use in deep fakes, or the delivery of lewd images or videos. In most cases, the law already addresses online harassment, including novel forms such as deep-fake videos and identity theft, or sharing non-consensual intimate imagery. However, these laws are jurisdictional and will have a limited impact in the Metaverse, calling for platform regulation. The scope of the Metaverse growing to include physical experiences through the neural link between the natural person's brain and their avatar in the Metaverse would complicate this further.[38]

Censorship

Another potential issue in the Metaverse is authority- and peer-enforced censorship and representation. User-centric social media platforms already have some form of authority-enforced censorship. The current online space is not as decentralised as the Metaverse aims to be, and so authorities can enforce some censorship based on their jurisdictions. While the internet allows for the easy transmission of misinformation and disinformation,[39] censorship does not automatically resolve these issues.[40]

Censorship must be approached neutrally in the Metaverse, where global citizens must be prioritised. The need to censor aspects that could harm users (such as medical misinformation) cannot be used as a carte blanche to censor speech that offends the sentiments of authorities.

Peer-enforced censorship—essentially, the restriction of users' freedom of expression by other users or non-authority figures—may also be unethical in the Metaverse. Peer-enforced censorship often occurs through griefing,[g] which can take the form of flaming,[h] trolling,[i] doxing,[j] and even virtual assault.[k,41] Since Web 3.0 is more secure in its authentication, requiring two-level authentication (such as one-time passwords, or links on one's personal email), and thus further protects digital speech beyond what current censorship can target, the onus for accountability and harassment mitigation is on users and platforms.[42]

g When users harass or abuse others in digital spaces
h Actively insulting or degrading another user.
i Instigating another user through insults or triggering words.
j Finding private information on a user and using the same against them, by publishing the information, or contacting them
k Verbal abuse motivated by a user's ethnicity, race, caste, religion, or gender, and can have physical outcomes.

Censorship can go beyond the restriction of speech, and can include the suppression of sexuality or the visual representation (even artistic and political representation) of such identities. Many countries continue to censor sexual representation,[43] and this could extend to the Metaverse as well.

To ensure users do not face any restrictions or harassment in how they choose to represent themselves, it is important to consider the ethics of avatar representation, expression, and the use of extended realities (XR).[l] Such considerations must be available 'in game' (i.e., applicable in games or offerings on different platforms) and 'on platform' (i.e., the commercial organisation that makes the offering). The ethics of what interactions enhance user experience versus what impacts user dignity must be discussed. XR is already being used for justice enforcement, such as VR being used to find sex offenders online, but such technologies have also been used nefariously, such as sex offenders using VR to locate vulnerable players on gaming platforms, and this can also happen in the Metaverse as well.[44,45] The Metaverse is being designed in a way that blurs the difference between real and virtual experiences for the user, increasing the user's susceptibility to embody the actions and experiences of their avatars, including verbal assault (also called the Proteus effect[m]).[46]

Each form of content, speech, or representation in the Metaverse that could potentially need to be censored will require a different approach. For example, misinformation and political free speech will require global alignment on what constitutes dissent and free speech. Censorship regarding gaming, social media interactions, and socio-personal displays like films and images will require platform-specific guidelines to protect minors and minority communities from abuse. The likelihood of these occurring in clearly defined spaces is low. Thus, overall regulations must also address how to govern a possible combination of such issues without necessarily banning users or removing access.

Decentralised Finance

The Metaverse will involve decentralised finance (DeFi)[n] that goes beyond national and physical currencies. The Metaverse's current gaming sector presents a preview of the possible economic and social implications of the DeFi landscape. Vast amounts of money are already being spent on the virtual

l Extended Realities (XR) includes augmented realities and virtual realities. It is a form of technology that adds to one's natural perception to help experience virtual stimuli.

m The Proteus effect describes a phenomenon in which the behaviour, thoughts, and actions of an individual are impacted and changed tangibly due to interactions in virtual worlds through thier avatars.

n A form of blockchain that is used to purchase or sell assets. Often referring to, but not limited to, cryptocurrency, it can also include smart contracts that require financial exchanges.

ownership of avatar skins and other gaming components;[47] for instance, the market for virtual skins was an estimated US$40 billion in 2022.[48] Additionally, gaming platforms also run play-to-earn games where users are paid in DeFi for their time. For instance, the number of participants for play-to-earn games like Axie Infinity increased from 30,000 to a million from April to August 2022.[49] While the use of DeFi is not inherently criminal, many countries account its volatility and lack of trackability to criminal activities like rug-pulling[o] and gold farming.[p,50]

This potential for expenditure and gain extends to other aspects of the Metaverse as well, and will result in the increased use of cryptocurrencies and other DeFi currencies.

Gaming platforms have created virtual real estate that has become desirable in the market, with users paying a reported US$450,000 for virtual land located next to other patches of virtual land owned by celebrities.[51] Virtual real estate is a rapidly growing industry alongside parallel businesses, such as virtual architecture and advisory firms. As in the physical world, price growth for these assets is driven by scarcity. This scarcity is encouraged by platforms like Decentraland and Sandbox, encouraging users to purchase virtual land, implying limited availability similar to real-world purchases. The lack of regulation in the purchase and selling of such 'land' adds to the volatility of prices, opening doors for DeFi-based exploitation.

Property rights (including intellectual property) and consumer protection in virtual ownership require regulation. The ownership of art, property, and technology is clearly understood in the physical world. In cyberspace, all property is intangible. With the introduction of NFTs, which allow the buyer to assume rights over a purchased product, distinguishing the intellectual property owner from the product owner is presently a matter of licensing. In some cases, the actual owner of intellectual property cannot resell the product without permission.[52] Consider, for instance, Hermes bags being converted to NFTs and sold without the company's permission.[53] As such, virtual real estate will also fall under the category of NFTs. This complicates regulating protections allowed to landowners, loans, or mortgages.

A further issue pertains to trading software that monitors cryptocurrency. If ML is involved, even programmed software can earn to trade in ways that lead to massive losses for investors. If losses occur based on learned behaviour that original programmers may not directly program, it would be unfair to assume liability to programmers.[54]

o Creating an asset of DeFi to attract buyers at an inflated price and shutting down the service/product once the purchase is complete.

p Gold farming refers to a user playing a game to purchase and resell in-game goods at a higher price.

The Need for Regulations in the Metaverse

Regulating the Metaverse is a challenge because it is still unclear exactly what form it will take once it has fully developed. The Metaverse's current aim is to be a decentralised platform not splintered by governments and local or regional jurisdictions. Nevertheless, given the potential for crime and criminal activity in the Metaverse, there is a need for global regulations pertaining to the Metaverse and its users. [55,56] The UN's Guiding Principles on Business and Human Rights outline the need to respect the privacy of an individual, and for businesses to adopt "best practices" as updated by regional and commercial alliances to ensure vulnerable classes (including gender, race and caste minorities) are protected. These guiding principles should be incorporated by all governments as a starting point in regulating the Metaverse.[57] However, the principles do not describe the nuances of business best practices, and so there is great scope to establish regulations specifically for the Metaverse. Some efforts are already underway worldwide.

In the EU, post the success of the General Data Protection Regulation (GDPR), the regulations for ensuring consumer protection and equitable competition, the Draft Digital Services Act[58] and Digital Markets Act[59] present new protections for minors that can be adopted into any future Metaverse regulation, including restricted access to illegal materials and decreased data storage for targeted advertising. Further, these regulations create an equitable landscape for different platforms, urging organisations to realign their marketing methods and remove push advertisements for their products. This, alongside reduced targeted advertising, helps address user privacy concerns, regulate markets, and remove unintentional oligopolies.[60] Similarly, the EU's Draft AI Regulation[61] creates new definitions and requirements for what qualifies as "high-risk" AI to make users less susceptible to marketing, data mining, and data storage.[62] This document also discusses preventing or restricting AI systems from harmful manipulative 'subliminal techniques'; AI systems that exploit specific vulnerable groups; AI systems used by public authorities, or on their behalf, for social scoring purposes; and 'real-time' remote biometric identification systems in publicly accessible spaces, except in a limited number of cases for law enforcement. While these are already helpful actions in the physical world, including provisions related to XR aspects of the Metaverse related to data collection and biometrics, such as eye movement data, will help set a foundation for future regulations.

The Need for Regulations in the Metaverse

In 2022, Japan announced the launch of its Web 3.0 Policy Office under the Ministry of Economy, Trade, and Industry to oversee all activities related to emerging social technology, including blockchain, NFTs, and the Metaverse.[63] Similarly, the UK has already said that Metaverse activities by commercial entities and users in the UK's jurisdiction will fall within the scope of its Online Safety Bill.[64]

The US, on the other hand, continues to rely on existing laws to govern the Metaverse, including the aspects of consumer protection and intellectual property, but it has not yet detailed Metaverse or Web 3.0 specific laws.[65,66]

In India, cybercrimes are covered by the Information Technology Act, 2000 (IT Act) and the Indian Penal Code, 1860.[67,68] India's cyber laws are more comprehensive than in many other countries with similar user bases,[69] and, as such, the country is in a suitable space to grow and establish primary versions of Metaverse regulations and ethical guidelines. A starting point would be to examine the existing relevant laws (such as the Indian Penal Code and IT Act)[70] and how their provisions can be applied to or altered for the Metaverse. For example, the IT Act has already been extended to include different forms of theft such as phishing[q] and cybersquatting.[r] These illegalities can extend to the Metaverse and address criminal behaviour such as rug-pulling, identity theft, and other forms of criminality where an online asset (including virtual avatars) is misused for purchases or to artificially inflate prices. India has also recently enacted the Digital Personal Data Privacy Act, which penalises individual users and organisations that do not comply with norms.[71] Similarly, penalties for non-compliance can be imposed on avatars in Metaverse without necessarily incriminating the individual user, in cases when the user or programmer are not directly responsible.

The Metaverse is primarily a user platform, whether the user is a human-controlled avatar, a company-created avatar for character merchandising, or an ML-based avatar used to enhance the platform experience. Regulating the Metaverse will need to be based on three principles: open and transparent governance; a strong focus on human rights; and public accountability (decentralised from any one nation).

q Acquiring another's data to use to steal their assets.

r Purchasing domain names with popular names to sell at a higher cost.

AI can allow for a fully automated functioning governance framework for the Metaverse. The outcomes of AI governance algorithms, however, can be biased and unfair, as they are still based on collective internet use and social interactions. A potential solution is developing a multilayered model for governance—the first layer of protection is based on data governance and algorithm accountability; the second layer guides decision-making and data processing via ethical criteria and norms; and the final social and legal layer addresses the allocation of responsibilities in regulation.[72]

Still, the development of a governance framework for the Metaverse must be collaborative to avoid the concentration of regulation rights with any one country. This can be done by creating a Metaverse monitoring entity in the United Nations or establishing a truly independent organisation beyond the existing global bodies.

As governments consider developing Metaverse-specific regulations, whether at a national or global level, the following aspects must be considered:

- **Granting avatars separate legal personalities**

The user is the primary priority in the Metaverse. One way to ensure that users are protected against other users hiding behind the anonymity of avatars or ML-enabled avatars is to grant them separate legal identities.[73] There are already discussions around attributing autonomy to AI.[74] Similar attributions can be extended to avatars, which would protect avatars from becoming scapegoats for users.[75,76]

- **Granting avatars rights akin to a company**

In the physical world, a registered company is treated differently than its stakeholders or proprietors. This concept of extended rights can also be attributed to avatars in the Metaverse. Like companies, avatars are non-human extensions of human activity.[77] Enabling avatars to act as companies would increase accountability on avatars, user-led and ML, encouraging acting more responsibly when interfacing in the Metaverse. [78]

These adjusted rights will also enable protections for companies, who may perform business activities as avatars while continuing to protect individual users.

- **Data privacy and protection**

The Metaverse will reflect present-day challenges regarding data privacy and intellectual property rights. Such problems are currently discussed and dealt with by existing intellectual property and consumer protection laws.

The current data protection rules, including India's Digital Personal Data Protection Act, the EU's GDPR and AI Act, and the US's Illinois Biometric Information Privacy Act,[s] do not account for the larger variety of biometric data that can be collected in the Metaverse. While most of the existing data protection laws cover static biometrics under sensitive or personal data, there is a gap regarding what can be derived from the dynamic movements or involuntary actions that may occur in the Metaverse.[79]

- **Human rights**

In a decentralised platform that currently lacks regulation, creating a protocol for assessing and protecting human rights is important. One way to do so is to create a policing and regulatory body or wing under Interpol, to oversee the Metaverse or create a strategy for its functioning. This body would not be accountable to any single government.[80]

- **Guidelines for ethical use**

The Metaverse may see a rise in severe side effects such as user addiction, biased outcomes, hearsay, and ineffective censorship.[81] As such, there should be ethical guidelines for using the Metaverse and its different offerings to ensure fair use and user protection. The UN's Guiding Principles on Business and Human Rights can guide the creation of Metaverse-specific rules by prioritising the protection of vulnerable sections of society and privacy and engaging commercial alliances to regularly update best practices.[82]

s The US does not have a federal regulation for biometric data. Only three states have regulations that include biometric-specific data privacy policies: Illinois, Washington DC, and Texas. The Illinois Act is the most comprehensive.

- **State security**

There is a possibility of the Metaverse being used to attack state infrastructure, such as the malware attacks on the Ukraine power grid in 2015[83] and NotPetya,[84] both of which have been linked to Sandworm.[t] In the Metaverse, with increased connectivity, such ransomware attacks may not be localised to one country or nationality. Potential regulations will need to be prepared for such instances as well.

> "Regulating the Metaverse is a challenge because it is still unclear exactly what form it will take once fully developed. The UN's Guiding Principles on Business and Human Rights—which outline the need to respect the privacy of an individual and for businesses to adopt "best practices" to ensure vulnerable sections of society are protected—should be incorporated by all governments as a starting point in regulating the Metaverse."

t A devastating cyberattack that has been alleged to Russian hackers, impacting Ukraine and many other countries, shutting down ports and other defense relevant systems.

Conclusion

The Metaverse is developing towards its final form, although what this will look like exactly is still unknown. Currently, the XRs offered by the Metaverse only expand on users' audio-visual experiences. However, if the anticipated stages of deeper immersion materialise, users will be more vulnerable to the products, services, and interactions hosted on the platform. Thus, addressing the potential for crime and misconduct—and how these can be regulated—is necessary before greater immersion can augment the scope of these wrongdoings.

The current regulatory landscape can provide the blueprint for governing the Metaverse. As the physical world increasingly blends with the virtual, user-safety-focused guidelines, particularly those relating to data privacy and responsible behaviour by organisations and individuals, can be expanded and evolved to include the various aspects of the Metaverse.

Shravishtha Ajaykumar *is Associate Fellow at ORF's Centre for Security Strategy and Technology.*

Endnotes

1 Josh Drake, "How We Can Finally Evolve from Web2 to Web3," *VentureBeat*, February 13, 2022, https://venturebeat.com/datadecisionmakers/how-we-can-finally-evolve-from-web-2-0-to-web-3-0/.

2 Edward Thomas, "Did Y2K Cause the Dot Com Crash?" February 27, 2017, https://www.edwardthomasauthor.com/single-post/2016/08/21/did-y2k-cause-the-dot-com-crash

3 Josh Drake, "How We Can Finally Evolve from Web2 to Web3."

4 Y Zhou et al., "Cyber-Physical-Social Systems: A State-of-the-Art Survey, Challenges and Opportunities," *IEEE Communications Surveys & Tutorials,* December 12, 2019, https://ieeexplore.ieee.org/document/8931796.

5 Henrique Centieiro, "The Roles of VR, AR and MR on the Metaverse," *Medium,* March 9, 2022, https://medium.datadriveninvestor.com/the-roles-of-vr-ar-and-mr-on-the-Metaverse-593569cfb686

6 McKinsey and Company, "Value Creation in the Metaverse," *McKinsey and Company*, June 2022, https://www.mckinsey.com/~/media/mckinsey/business%20functions/marketing%20and%20sales/our%20insights/value%20creation%20in%20the%20Metaverse/Value-creation-in-the-Metaverse.pdf.

7 "Haptic VR Suit and Glove with Force Feedback," *Teslasuit,* June 29, 2022, https://teslasuit.io/.

8 Henrique Centieiro, "The Roles of VR, AR and MR on the Metaverse."

9 "Fingerprint, Face, Eye Iris, Voice and Palm Print Identification, Speaker and Object Recognition Software," *Neurotechnology,* June 27, 2022, https://www.neurotechnology.com/.

10 Shahnaz Shahrbanian et al., "Use of Virtual Reality (Immersive vs. Non Immersive) for Pain Management in Children and Adults: A Systematic Review of Evidence from Randomized Controlled Trials," *European Journal of Experimental Biology* (2012), https://www.researchgate.net/profile/Shahnaz-Shahrbanian/publication/315740184_Use_of_virtual_reality_immersive_vs_non_immersive_for_pain_management_in_children_and_adults_A_systematic_review_of_evidence_from_randomized_controlled_trials/links/5a340974a6fdcc769fd22817/Use-of-virtual-reality-immersive-vs-non-immersive-for-pain-management-in-children-and-adults-A-systematic-review-of-evidence-from-randomized-controlled-trials.pdf.

11 Neuralink, "Potential Impact," *Neuralink,* https://neuralink.com/.

12 Henrique Centieiro, "The Roles of VR, AR and MR on the Metaverse."

13 Wang et al., "A Survey on Metaverse: Fundamentals, Security, and Privacy," *TechRxiv,* March 6, 2022, https://doi.org/10.36227/techrxiv.19255058.v1.

14 McKinsey and Company, "Value Creation in the Metaverse."

Endnotes

15 McKinsey and Company, “Value Creation in the Metaverse.”

16 Osman Gazi Gucluturk, "The Role of the Law in Metaverse Regulation," *Metaverse: Technologies, Opportunities and Threats* (2023), https://link.springer.com/chapter/10.1007/978-981-99-4641-9_18.

17 Shravishtha Ajaykumar, “Gender-Based Violence in Private Online Spaces,” *Observer Research Foundation*, June 23, 2022, http://20.244.136.131/expert-speak/gender-based-violence-in-private-online-spaces.

18 Vikram Rao et al., “To Share or Not to Share,” *Deloitte Insights*, September 25, 2017, https://www2.deloitte.com/us/en/insights/industry/retail-distribution/sharing-personal-information-consumer-privacy-concerns.html.

19 Morgan Stanley, “Should Investors Take the Metaverse Seriously?” *Morgan Stanley*, November 14, 2021, https://www.morganstanley.com/ideas/Metaverse-investing.

20 Bhavishya Ravi, "Privacy Issues in Virtual Reality: Eye Tracking Technology." *Bloomberg Law* (2017). https://www.academia.edu/download/77883748/Privacy_Issues_in_Virtual_Reality_Eye_Tracking_Technology.pdf.

21 Matthew Gault, “The Metaverse Is the Ultimate Surveillance Tool,” *VICE*, November 12, 2021, https://www.vice.com/en/article/bvnxbm/the-Metaverse-is-the-ultimate-surveillance-tool.

22 Guohao Lan et al., “Eyesyn: Psychology-Inspired Eye Movement Synthesis for Gaze-Based Activity Recognition,”*2022 21st ACM/IEEE International Conference on Information Processing in Sensor Networks* (2022), https://maria.gorlatova.com/wp-content/uploads/2022/03/EyeSyn_CR.pdf.

23 Kate Crawford, “Artificial Intelligence is Misreading Human Emotion,” *The Atlantic*, April 27, 2021, https://www.theatlantic.com/technology/archive/2021/04/artificial-intelligence-misreading-human-emotion/618696/.

24 Ernst and Young, “Insights on the Metaverse and the Future of Gaming.” *Ernst and Young*, 2022, https://www.ey.com/en_us/tmt/what-s-possible-for-the-gaming-industry-in-the-next-dimension/chapter-3-insights-on-the-metaverse-and-the-future-of-gaming.

25 Andrea Vittorio, “Metaverse Technology Opens Up a Wider World of Privacy Concerns,” *Bloomberg Law*, August 30, 2022, https://news.bloomberglaw.com/privacy-and-data-security/metaverse-technology-opens-up-a-wider-world-of-privacy-concerns.

26 Thomas Macaulay, “Why Emotion Recognition AI Can't Reveal How We Feel,” *TNW | Neural*, August 23, 2021, https://thenextweb.com/news/emotion-recognition-ai-cant-determine-how-people-feel.

27 Isobel Asher Hamilton, “Meta Wants to Track Your Eye Movements and Facial Expressions as You Roam the Metaverse, Patents Suggest,” *Business Insider*, January 18, 2022, https://www.businessinsider.in/tech/news/meta-wants-to-track-your-eye-movements-and-facial-expressions-as-you-roam-the-Metaverse-patents-suggest/articleshow/88977447.cms.

Endnotes

28 Klein et al., "Pathways to Conspiracy: The Social and Linguistic Precursors of Involvement in Reddit's Conspiracy Theory Forum," *PLoS ONE,* November 18, 2019, https://doi.org/10.1371/journal.pone.0225098.

29 Pin Lean Lau, "From Data to User Interactions: Legal Issues Facing the Metaverse," *The Fashion Law,* February 2022, https://www.thefashionlaw.com/from-data-to-user-interactions-legal-issues-facing-the-Metaverse/.

30 "Metaverse in Gaming Market Share, Forecast: Growth Analysis Opportunities [2023-2031]," *MarketsandMarkets*, https://www.marketsandmarkets.com/Market-Reports/metaverse-in-gaming-market-15811534.html#:~:text=The%20Metaverse%20in%20Gaming%20Market,projected%20to%20reach%20%24119.2%20billion.

31 Mary Anne Franks, "Unwilling Avatars: Idealism and Discrimination in Cyberspace," *Columbia Journal of Gender and Law, Vol. 20*, October 21, 2009, https://ssrn.com/abstract=1374533.

32 "Character Merchandising," *WIPO – World Intellectual Property Organization,* December 1994, https://www.wipo.int/export/sites/www/copyright/en/docs/wo_inf_108.pdf.

33 J.J. Bryson et al., "Of, For, and By the People: The Legal Lacuna of Synthetic Persons," *Artificial Intelligence and Law*, September 8, 2017,https://doi.org/10.1007/s10506-017-9214-9.

34 Danielle Garno, "Trademarks Meet NFTs: Hermès Sues NFT Creator Over MetaBirkins," *Reed Smith*, January 26, 2022, https://www.adlawbyrequest.com/2022/01/articles/in-the-courts/trademarks-meet-nfts-hermes-sues-nft-creator-over-metabirkins.

35 Rahul Sharma, "Case Summary: Lee vs. Lee Air Farming Limited, 1960," *LawLex.Org*, July 15, 2020, https://lawlex.org/lex-bulletin/case-summary-lee-vs-lee-air-farming-lee-limited-1960/24542.

36 B.C. Cheong, "Avatars in the Metaverse: potential legal issues and remedies," *International Cybersecurity Law Review*, June 7, 2022, https://doi.org/10.1365/s43439-022-00056-9.

37 B.C. Cheong, "Avatars in the Metaverse: potential legal issues and remedies."

38 B.C. Cheong, "Avatars in the Metaverse: potential legal issues and remedies."

39 Rachel Schraer, "Should Bad Science Be Censored on Social Media?" *BBC News*, January 19, 2022, https://www.bbc.com/news/technology-60036861.

40 Rachel Schraer, "Should Bad Science Be Censored on Social Media?" *BBC News*, January 19, 2022, https://www.bbc.com/news/technology-60036861.

41 "How I Temporarily Became a Griefer," *VentureBeat*, July 24, 2012, https://venturebeat.com/gbunfiltered/how-i-temporarily-became-a-griefer/.

42 Arne Hintz, "Social Media Censorship, Privatized Regulation and New Restrictions to Protest and Dissent," *Critical perspectives on social media and protest: Between control and*

Endnotes

emancipation (2015), https://books.google.co.in/ks?hl=en&lr=&id=iOHaDwAAQBAJ&oi=fnd&pg=PA109&dq=peer+reporting+censorship+on+decentralised+social+media&ots=G8bDJbZOI9&sig=6Z0yaPrpNgh3vfn756_qRKNNk7A#v=onepage&q&f=false.

43 Elizabeth Picarra, "Avatars and Virtual Worlds: Unsettling the Rules of Porn," *Empowering Women for Gender Equity*, October 29, 2022, https://www.jstor.org/stable/pdf/43824480.pdf?ab_segments=0%2Fbasic_search_gsv2%2Fcontrol&initiator=search-results.

44 Matt Roper, "Predators Use Virtual Reality Chatroom to Target Kids on Popular Gaming Device," *Mirror,* February 9, 2022, https://www.mirror.co.uk/news/uk-news/predators-use-virtual-reality-chatroom-26186533.

45 Nina Jane Patel, "Fiction vs. Non-Fiction," *Medium*, February 4, 2022, https://medium.com/kabuni/fiction-vs-non-fiction-98aa0098f3b0.

46 N. Yee et al., "The Proteus Effect: Implications of Transformed Digital Self-Representation on Online and Offline Behavior," *Communication Research,* January 22, 2009, http://dx.doi.org/10.1177/0093650208330254.

47 "Cryptocurrencies Are on Track to Dominate Online Video Gaming," *Medium,* March 19, 2018, https://medium.com/wax-io/cryptocurrencies-are-on-track-to-dominate-online-video-gaming-and-here-are-the-numbers-that-show-cbe81dc397b0.

48 Matthew Petkov, "How Virtual Fashion is Changing the Industry," *LandVault* May 30, 2023, https://landvault.io/blog/virtual-fashion

49 "Unemployed Gamers Turn to Crypto Game Axie Infinity to Make Hay," *The Times of India,* August 30, 2021, https://timesofindia.indiatimes.com/business/cryptocurrency/etherum/unemployed-gamers-turn-to-crypto-game-axie-infinity-to-make-hay/articleshow/85760211.cms.

50 Amanda Holpuch, "Gaming Is Booming. That's Catnip for Cybercriminals," *The New York Times*, October 13, 2022, https://www.nytimes.com/2022/10/13/technology/gamers-malware-minecraft-roblox.html.

51 "Crypto Collector Spends $450,000 on Land Next to Snoop Dog," *The Express Tribune*, December 9, 2021, https://tribune.com.pk/story/2333136/crypto-collector-spends-450000-on-virtual-land-next-to-snoop-dogg.

52 B.C. Cheong, "Avatars in the Metaverse: potential legal issues and remedies."

53 Danielle Garno, "Trademarks Meet NFTs: Hermès Sues NFT Creator Over MetaBirkins."

54 Mark Coeckelbergh, "Artificial Intelligence, Responsibility Attribution, and a Relational Justification of Explainability," *Science and Engineering Ethics*, October 24, 2019, https://link.springer.com/article/10.1007/s11948-019-00146-8.

55 Dan York, "What Is the Splinternet? And Why You Should Be Paying Attention." *Internet Society*, March 28, 2022, https://www.internetsociety.org/blog/2022/03/what-is-the-splinternet-and-why-you-should-be-paying-attention/.

Endnotes

56 Louis B. Rosenberg, "Regulating the Metaverse, a Blueprint for the Future," *Lecture Notes in Computer Science*, August 26, 2022, https://link.springer.com/content/pdf/10.1007/978-3-031-15546-8_23.pdf.

57 Office of the High Commissioner for Human Rights, United Nations, "Guiding Principles on Business and Human Rights," *Office of the High Commissioner for Human Rights*, June 16, 2011, https://www.ohchr.org/sites/default/files/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

58 Parliament, European Union, "Digital Services Act," *European Parliament*, December 15, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0825.

59 Parliament, European Union, "Digital Markets Act," *European Parliament*, October 19, 2022, https://digital-markets-act.ec.europa.eu/index_en.

60 Shravishtha Ajaykumar, "Democratising the Internet," *Observer Research Foundation*, September 28, 2022, https://www.orfonline.org/expert-speak/democratising-the-internet/.

61 Parliament, European Union, "Artificial Intelligence Act" *European Parliament*, January 14, 2022, https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)698792#:~:text=The%20European%20Commission%20unveiled%20a,AI%20systems%20and%20associated%20risks.

62 Laura De Boel, "Council of the EU Proposes Amendments to Draft AI Act," *Wilson Sonsini*, December 22, 2022, https://www.wsgr.com/en/insights/council-of-the-eu-proposes-amendments-to-draft-ai-act.html.

63 Paul Bond, "EU, South Korea, Japan Announce Metaverse Regulation Plans," *Holland & Knight Masters of the Metaverse*, https://www.hklaw.com/en/insights/publications/2022/09/eu-south-korea-japan-announce-metaverse-regulation-plans.

64 UK Parliament, Government of the United Kingdom of Britain, "Online Safety Bill - Parliamentary Bills - UK Parliament," *UK Parliament*, June 26, 2023, https://bills.parliament.uk/bills/3137.

65 "What Laws Govern the Metaverse?" *Blockchain Council*, January 16, 2023, https://www.blockchain-council.org/metaverse/what-laws-govern-the-metaverse/.

66 Nisa Amolis, "How Regulation will Apply to The Metaverse," *Forbes*, March 1, 2023, https://www.forbes.com/sites/alexkonrad/2023/06/29/inflection-ai-raises-1-billion-for-chatbot-pi/?sh=64df13461d7e.

67 Government of India, "The Indian Penal Code Arrangement of Sections," *Government of India*, https://legislative.gov.in/sites/default/files/A1860-45.pdf.

68 Government of India, "The Information Technology Act, 2000," *Government of India*, https://www.indiacode.nic.in/bitstream/123456789/13116/1/it_act_2000_updated.pdf.

Endnotes

69 Christian Laue, "Crime Potential of Metaverses," *Virtual Worlds and Criminality (pp.19-29)*, August 2011, https://www.researchgate.net/publication/226170289_Crime_Potential_of_Metaverses.

70 Ministry of Corporate Affairs, Government of India, "Offences and Penalties" *Government of India*, https://www.mca.gov.in/MinistryV2/offences+and+penalties.html.

71 Ministry of Law and Justice, Government of India, "The Digital Personal Data Protection Act, 2023," *Ministry of Law and Justice*, https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf.

72 Gasser et al., "A Layered Model for AI Governance," *IEEE Internet Computing*, November 20, 2017, https://ieeexplore.ieee.org/document/8114684.

73 S. M. Solaiman, "Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy," *Artificial Intelligence and Law*, July 16, 2017, https://ro.uow.edu.au/lhapapers/3076/.

74 Simon Chesterman, "Artificial Intelligence and The Problem of Autonomy," *NUS Law Working Paper Series*, September 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3450540.

75 S. M. Solaiman, "Legal Personality of Robots, Corporations, Idols and Chimpanzees: A Quest for Legitimacy."

76 Matt Roper, "Predators Use Virtual Reality Chatroom to Target Kids on Popular Gaming Device."

77 Tiffany Day, "Avatar Rights in a Constitutionless World," *Hastings Communications and Entertainment Law Journal* (2009), https://repository.uchastings.edu/hastings_comm_ent_law_journal/vol32/iss1/5/.

78 Bryant Smith, "Legal Personality," *Yale Law Journal*, January 1928, https://openyls.law.yale.edu/bitstream/handle/20.500.13051/12065/23_37YaleLJ283_1927_1928_.pdf.

79 "Biometric Data and Privacy Laws (GDPR, CCPA/CPRA)," *Thales Group*, June 16, 2021, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/biometrics/biometric-data.

80 Jayanth Murali, "Should We've Virtual Version of Interpol to Police the Metaverse?" *DT next*, January 9, 2022, https://www.dtnext.in/technology/2022/01/09/should-weve-virtual-version-of-interpol-to-police-the-Metaverse.

81 Wang et al., "A Survey on Metaverse: Fundamentals, Security, and Privacy," *IEEE Communications Surveys & Tutorials*, September 8, 2022, https://arxiv.org/abs/2203.02662v2.

82 Office of the High Commissioner for Human Rights, United Nations, "Guiding Principles on Business and Human Rights."

Endnotes

83 Don C. Weber, "Confirmation of a Coordinated Attack on the Ukrainian Power Grid," *SANS Industrial Control Systems Security*, May 6, 2021, https://www.sans.org/blog/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid/.

84 Andy Greenberg, "The Untold Story of Notpetya, the Most Devastating Cyberattack in History," *Wired*, August 22, 2018, https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/.

Images used in this paper are from Getty Images/Busà Photography.

ORF OBSERVER RESEARCH FOUNDATION

Ideas . Forums . Leadership . Impact

20, Rouse Avenue Institutional Area,
New Delhi - 110 002, INDIA
Ph. : +91-11-35332000. **Fax :** +91-11-35332005
E-mail: contactus@orfonline.org
Website: www.orfonline.org